Best Practices for the Handling of Electronic Evidence

State of Maryland

Introduction

In an effort to increase the overall statewide security capabilities, the State of Maryland has contracted SAIC to provide assistance in developing and implementing a comprehensive statewide security program. This effort consists of four primary taskings including the development of a statewide Incident Response capability. An integral part of this capability is the proper handling of electronic evidence when investigating any incident.

Purpose

This presentation will identify best practices for collecting, handling and maintaining various forms of electronic evidence when responding to an incident. These best practices represent a subset of the overall Incident Response Methodology found in the document titled State of Maryland Security Incident Response Capability (IRC) Plan, Document Control Number: SAIC-6099-2002-088. This document was developed to ensure consistency in incident handling procedures throughout the state.

Policy / Authorization

The Maryland Code, Law Pertaining to Information Processing, State Finance and Procurement, Title 3, Subtitle 4, 3-401 to 3-413 authorizes this capability. Section 3-403 (a) charges the Secretary, DBM, with responsibility "for developing, maintaining, revising, and enforcing information technology policies and standards." Section 3-410 authorizes the Chief of Information Technology (also known as the State CIO) to carry out certain duties for the Secretary, DBM. Section 3-410 (d) (1) charges the Chief to be responsible to the Secretary DBM for carrying out the duty of "developing, maintaining, and enforcing statewide information technology standards, policies, and procedures." The State CIO has created the Security and Architecture Division within the Office of Information Technology of the Department of Budget and Management to assist the State CIO. The Deputy Director for Security of the Security and Architecture Division has caused this capability to be implemented.

Recognizing Digital Evidence

Investigation of any kind may produce digital evidence if electronic devices are used to generate, store or transport information relating to an incident. The role of the electronic Evidence can be determined by answering the following:

1. Is the electronic evidence contraband of the fruits of an incident? (I.e. Was the electronic evidence stolen)
2. Is the electronic evidence a tool for the incident? (i.e. Was the electronic evidence used to commit the incident)
3. Is the electronic evidence incidental to the offense? (i.e. Is the electronic evidence being used to collect pictures to be stored on a computer)
4. Is the electronic evidence instrumental to the offense, and an ancillary storage medium for an offense?

Computer Systems

Computer Systems - Considerations

1. If a system is being considered for collection, the state of the system should be the first consideration. Attempts to log into a system in standby mode, bring a system out of a state of hibernation, or "properly" shut down using normal operating system methods may result in writing entries into the log or registry files thus changing the contents of the drive (and evidence) significantly. Computer systems should be first photographed for documentation, and then turned off at a switch, plug or other power source to prevent unnecessary changes from occurring. If the system is connected to a network, care should be taken to ensure that it is not being used as a server or other processing resource.

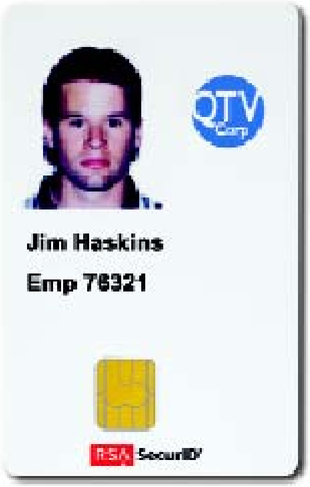
2. Systems containing potential evidence should be identified and shut off prior to removing any peripherals plugged into the system. This will also ensure that entries are not written to the log pertaining to changes in hardware.

3. Any media should remain intact if the system is able to be removed as evidence. External media bays should be sealed with evidence handling tape, and documented with the collector's signature and the date and time of removal.

4. When removing any internal drives, any connections should be properly sealed and documented to prevent unauthorized tampering. Drive settings should remain unchanged including jumper settings and write protection.

5. Input devices should remain with computer systems to ensure compatibility when provided to the incident response team for analysis.

Authentication Devices



Authentication Devices - Considerations

1. Access control devices may or may not be stored with the systems or devices that they provide access to.

2. Batteries that have a finite life expectancy commonly power access control devices.

3. Typical access control devices interact with software residing on the system(s) being accessed.

4. There are three types of access control mechanisms based on security considerations. Single factor devices rely on one type of information for access control (something known such as passwords or pass codes), two factor authentication devices rely on two types of information to authenticate a user (something known and something possessed like smart cards), and three factor devices relate to three pieces of information for authentication (something known, something possessed, and something inherent to the user like biometrics).

Digital Cameras

(Memory Stick® Media Sold Separately)

Digital Cameras - Considerations

1 Images produced by a digital camera are typically stored on compact volatile magnetic or optical media and stored either within the device, or separate from the device. Images produced with the camera may also be off-loaded to systems or media as back up or storage as the compact media is limited in size.

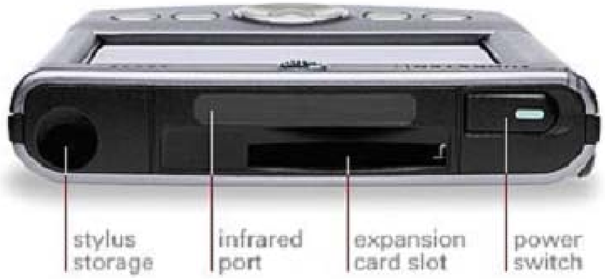
2 Cameras depend on batteries and often have charging docks that provide recharging.

3 Cameras typically have various interfaces for connecting to various system ports, television and multimedia devices.

4 Additional media readers may be present on systems or printers for off-loading pictures for storage or output.

5 Some digital cameras, sometimes referred to as web cams, are mounted on the monitor or desktop and connected directly to a computer system providing a camera capability for Internet use. These web cams store information on the systems drives and should be considered a peripheral to the system.

Handheld Digital Devices / PDAs



Handheld Digital Devices/PDAs - Considerations

1 These devices typically synchronize with a host computer system, or multiple host systems. Content available on these devices may represent a subset, a replica, or a conglomeration of information from one or various other electronic sources.

2 Power for these devices is typically provided through batteries. Some use rechargeable cells, where others use disposable cells. It should never be assumed that the information will remain during long periods without battery operation.

3 Battery chargers, cradles and system interfaces are commonly found on systems used as hosts to these devices. All of these should be collected as evidence with the device.

4 Many handheld electronic PDAs have automatic power-up functionality when alarms are set. Care should be taken to ensure that the device is turned off, the infrared port (if available) is properly covered with an opaque tape, and the cover is sealed to prevent contamination of data.

5 Many PDAs have wireless modems that allow access to Internet, email and other remote functions.

6 PDAs storage may be used to store files, documents, mail and other forms of digital media from the host system(s).

Electronic Organizers

Electronic Organizers- Considerations

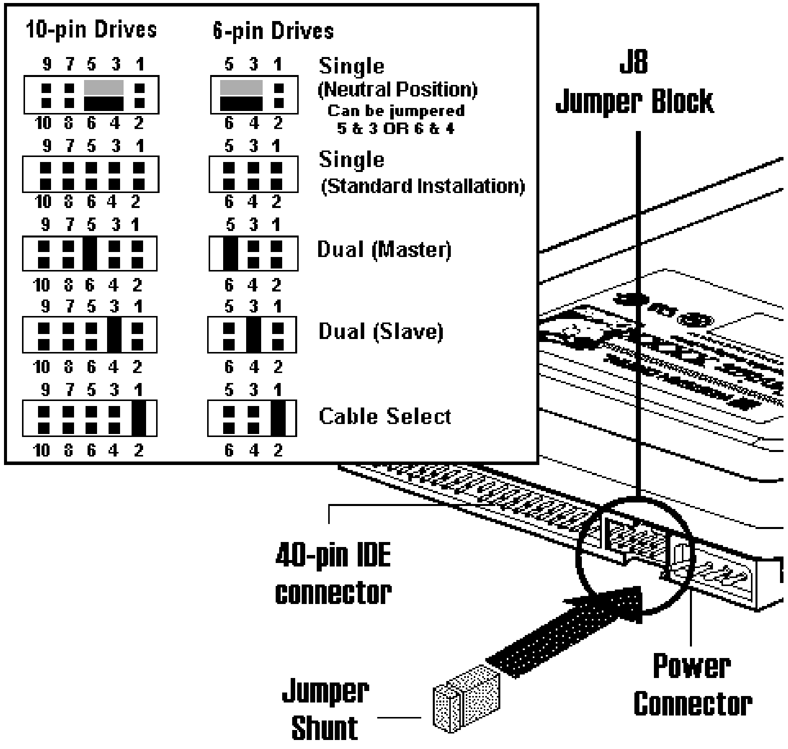
1 These devices usually operate on battery power. Information is typically volatile and should be considered at risk if battery power subsides.

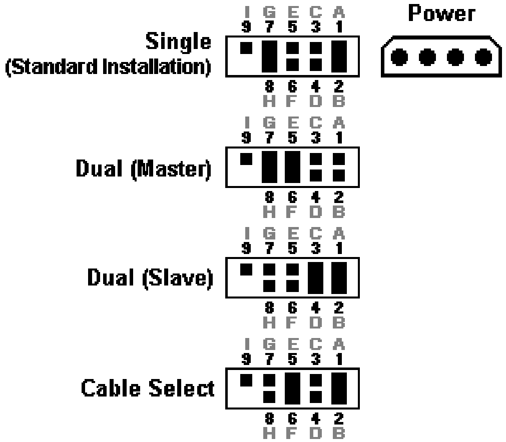
2 These items may be found remote from any systems being collected and may not provide connectivity to host systems.

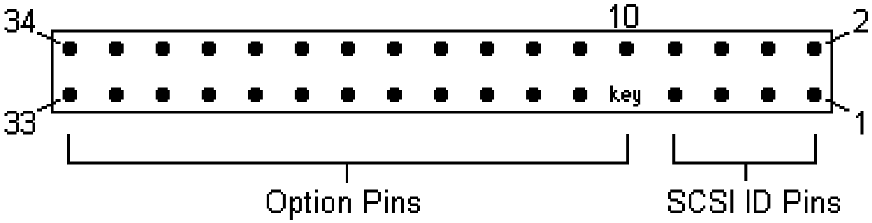
3 Organizers typically have non-removable internal storage with very limited capacity.

4. Organizers operating systems are typically proprietary and restrictive. Access to storage fields is likely limited to the fields designed for that particular device. Rarely are the drives on these devices used to store data from other hosts.

Hard Drives


10-pin Drives
6-pin Drives
9 7 5 3 1
10 8 6 4 2
5 3 1
6 4 2
Single
(Neutral Position)
Can be jumpered
5 & 3 OR 6 & 4
Single
(Standard Installation)
Dual (Master)
Dual (Slave)
Cable Select
J8
Jumper Block
40-pin IDE
connector
Jumper
Shunt
Power
Connector


Power
I G E C A
9 7 5 3 1
8 6 4 2
H F D B
Single
(Standard Installation)
Dual (Master)
Dual (Slave)
Cable Select


34
10
2
33
key
1
Option Pins
SCSI ID Pins

Hard Drives - Considerations

1 Hard drives require a host system to function. The system provides power, software, and functionality through a specific type of interface.

2 Hard drives may be designed for IDE interfaces or SCSI interfaces.

3 Jumper settings should remain intact. These settings are designed to ensure that multiple drives can be used on one system (primary or slave) and their setting may represent evidence.

4 Drive dimensions for laptop drives tend to be smaller than desktop systems. The interface used to connect these drives also differs in size and configuration.

5 Hard drives are considered magnetic media and should remain away from any magnetic field that may cause destruction of data.

6 Ribbon cables should be removed from drive interfaces with care as “pins” tend to be delicate.

7. Drive casings should never be removed as this may cause damage to the cylinders and tracks, and cause the drive to not function properly.

Memory Cards

Memory Cards - Considerations

1 Memory cards typically come in compact cards or “sticks” depending on the manufacturer.

2 Memory cards typically come in sizes ranging from 4, 8 16,32,64 or 128 MB.

3 Newer memory cards look like key chains and store information similar to a hard drive. These devices come apart and plug into the USB interface on a computer system.

4 Memory cards are considered “removable media” an require other electronic devices for power and to function.

5. Memory cards may be used to store any information found on a computer system including music, video, images, documents, or data.

Modems

Actiontec

Broadband Cable Modem
NETGEAR

USB modem

56 FAX/Modem
Kbps
PC Card
Fax
Modem
PCMCIA
CNet

Modems - Considerations

1 Modems may be internal or external to the electronic device.

2 Modems may connect to telephone lines, cable lines, or wireless antennas to allow electronic devices to communicate.

3 External modems typically require an external power source and operate as a peripheral to a computer system using a variety of interfaces.

4 Modems operate at varying speeds.

5. Inclusion of a telephone modem in a corporate setting may indicate that an analog line exists, as modems require analog lines to communicate. This should be included as evidence if found present.

Networked Components

Networked Devices - Considerations

1 A network component may be servicing multiple electronic devices. Care should be taken to understand what devices are connected to the network component to ensure that users external to an investigation are unaffected.

2 Many times a network device will not be movable due to operational considerations. In this case, the relevant evidence must be extracted from the device using a sound forensic methodology (which is beyond the scope of this document).

3 Many network devices are wireless and may appear disconnected.

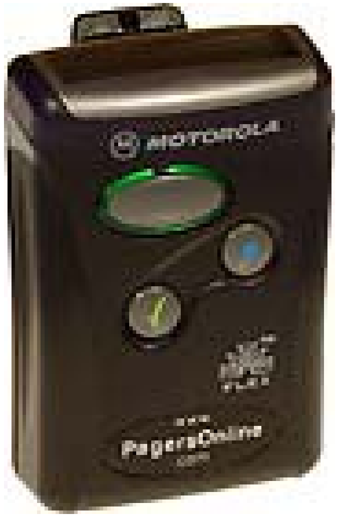
4 Network devices should not be disconnected until the main power to the host device is off. This will ensure that evidence on the host device is preserved.

5. Some computer systems and electronic devices have infrared ports that allow networking to other systems or devices. These ports should be considered network components and secured with opaque tape to ensure evidentiary integrity of the host system.

Pagers

MOTOROLA
www.PagersOnline.com

MOTOROLA
Read
TIMEPORT


MOTOROLA
PagersOnline

Pagers - Considerations

1 Most pagers operate on disposable or rechargeable batteries. Since batteries have a limited life, data could be lost if they fail. Therefore, a device powered by batteries is in need of immediate attention.

2 Information identified on the screen of a pager should be photographed, as it may not be stored when the device is turned off.

3 The pager may provide numeric or alphanumeric information and may provide either one-way or two-way communications.

4. Pagers often have identification information (i.e. Pin Number) on the outside case. This should be examined and photographed if possible.

Printers

Printers - Considerations

1 Printers may be connected locally or through a network or wireless type connection.

2 If a local connection exists, the printer may be connected to the host system through either a parallel cable or a USB cable.

3 If the printer is networked, it provides services for multiple clients and removal may disrupt service to other users.

4 Networked printers will either be connected to a print server or a network printing device such as Hewlett Packard’s Jet Direct Card. These devices should be considered for inclusion as evidence if present.

5. Some devices contain infrared ports allowing printing to occur without a cabled connection to the printer. Care should be taken to ensure that the infrared port is adequately covered with opaque tape to prevent unintentional access or contamination of evidence.

Removable Storage

Removable Storage - Considerations

1 As removable media depends on the appropriate storage device for operation, it is important to include these devices in an evidentiary collection to ensure proper access.

2 Some optical media such as CDRs written with Roxio’s Direct CD are written for use only with the specific device used to create the CD.

3 Some types of removable media are magnetic and may be destroyed if contact with other magnetic fields is made. Care should be taken to keep all electronic media away from speakers, magnets and electric motors.

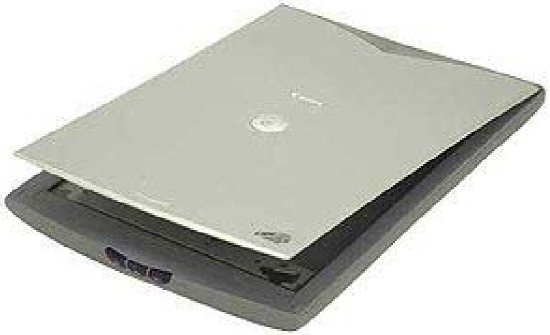
4 Many forms of removable media have write protection mechanisms on the surface to protect accidental erasure or overwrite. The status of these mechanisms should be documented and remain unaltered for analysis.

5 Most removable media has protective cases and labels that may prove useful in an investigation. These may or may not contain the media and should not be overlooked.

6. Removable media stored in a system being collected as evidence should remain in the unit and sealed with evidence tape.

Scanners

Quick Link
aaaaaaaaaaaa|~ ~ Hair
Blonde H azel 12/12/
1992 3-4925 Kle BIZ
ENT



CASIO
READING
START/STOP
ON/OFF
READ TYPE
SET UP
MODE
SET
Freedio
GILBERT
Planning Department
CASIO COMPUTER CO., LTD.

PF 1800

Scanners - Considerations

1 Scanners may be found as flatbed or handheld variants.

2 Scanners are often found in all-in-one office appliances providing printing, copying and fax capabilities.

3 Scanners typically attach to a local port on a computer system through a cable. Types and lengths of cable may vary based on location and type of scanner.

4. Many scanners utilize Optical Character Recognition (OCR) software allowing editing of physical documents with word processors.

Phones

T720i

Dave Jordan
2345
Meridian
Hold
Rls
Handsfree
Pick Up
Speed Call
Group Call
Park
Auto Ans
Auto Dial
Display
Program
Ring Again
Forward
Message
Transfer
Conference
2345
2616
<<<
>>>

Phones - Considerations

1 Most business facilities offer phone services to employees through a centrally controlled switch. Phones tend to be digital and all logs, records and configuration files are stored on the switch.

2 Cellular users may store information locally. Cellular phones operate on battery power and may or may not retain information once the battery wears out.

3 Cellular phones come in two varieties; IS41 that contain all user al information within the physical handset, and GSM which store all user operational information in a smart card or chip. US phones are typically IS41, but frequent travelers may have GSM or hybrid variants.

4 Some phones provide advance functionality through wireless internet access. Additional services may include web surfing, email, web calendaring and internet contact lists.

5 Some cellular phones have infrared ports to synchronize with various electronic devices including PDAs, computer systems, and handheld organizers.

6 Phones that are not part of a centrally located switch are typically analog and may have additional input interfaces for data. These types of phones typically store personal information in a small internal storage capacity.

7. Additional devices used for performing identification of incoming calls (CallerID) may also be available to provide historical records of incoming phone activity.

Miscellaneous Devices and Accessories

Miscellaneous - Considerations

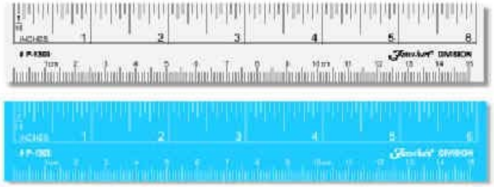
1 As a rule of thumb, any electronic device, item that supports an electronic device, or item created using an electronic device may be collected under this category.

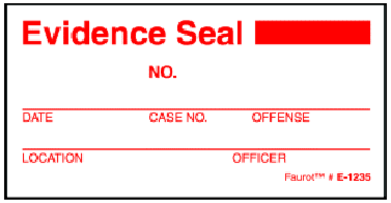
2 After collecting all of the relevant devices available, it is important to ensure that any support items are included to ensure that data can be retrieved for analysis. Items such as power supplies, PCMCIA cards and dongles, interface cables, input devices, docking stations and port replicators should be included with the supported devices.

3 Paper output should be collected if produced on printers, fax machines or adding tapes previously collected as evidence.

4. Other electronic devices such as micro recorders, calculators and dictation devices may also add information relevant to an investigation.

Evidence Collection Tools



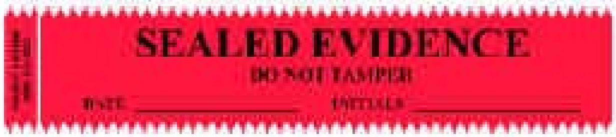

Evidence Seal

NO.

DATE CASE NO. OFFENSE

LOCATION OFFICER

Faurot™ # E-1235


SEALED EVIDENCE

DO NOT TAMPER

DATE ____________ INITIALS ____________

Documentation

1. The name, title and location for the evidence collector

2. The date and location the evidence is being collected from

3. A complete description of each item to be included into evidence including make, model, serial number, capacity (if known), quantity, and descriptions of any visual details that are noticed.

4. Pictures of all items are recommended to ensure consistence before and after collection. These pictures may include various angles, screen shots and general site shots for documentation.

5. A description of the process used to disengage, disassemble and package any electronic evidence providing a time based account of any activity pertaining to the collection. This should include timestamps when each action was taken.

Storage and Transport Requirements

1. When evidence is collected, various photographs are important not only to document a before and after state, but also to ensure proper setup for examination and assessment. In order to ensure investigative integrity, proper (same as original) cable placement is imperative. Additional steps to ensure proper evidence handling are colored stickers matching cables to interfaces, various sized plastic bags to hold smaller media, and adhesive tabs for identifying any observable damage or anomalies.
2. All digital evidence should be sealed in a proper sized carton, bag or envelope and packed tightly with foam, paper or other forms of non abrasive packaging materials to ensure damage free transport.
3. Any open storage bays should be occupied by either a safe transport media device, or blank media designed for the particular drive. This will ensure that the heads of the drive are parked during transport to avoid damage.
4. A detailed inventory worksheet (Appendix A and B) should accompany any evidence stored in a single carton, bag or envelope. This inventory should be signed by the collector, and verified once opened by an authorized responder.
5. All cartons, bags and envelopes should be sealed with heavy-duty reinforced packaging tape and signed and dated using a permanent marker, or forensic evidence tape can be purchased for this requirement.

Storage and Transport Requirements (Cont'd.)

6. Each carton, bag or envelope should be labeled with the words "FRAGILE" and "HANDLE WITH CARE". This will hopefully prevent damage if the items are being shipped to the destination, or are handled by others. Any deviations in handling should be fully documented for chain of custody.

7. Items being transported by collector should remain in his/her possession at all times. If third party shipping methods are used, the cartons should be properly labeled and numbered. If third party shipping is being used (Not recommended if avoidable), collectors should remain in possession of packages until physically received by shipping authority. If possible, a signature of possession should be obtained from shipping authority.

8. Once delivered to site of destination, cartons should always be properly examined for damage, evidence of tampering, or other anomalies not present at the site of origin. Observations should be recorded. If possible, pictures of boxes should be taken showing integrity of carton and seal.

9. When opening carton, bag or envelope, care should be taken if using sharp instruments. Sealing tape should remain on package to preserve evidence of process. Never remove sealing tape from package.

10. Items contained in packages should be verified against the accompanying inventory listing. Care should be taken to ensure that all information matches package contents (i.e. Serial Number, Make Model…) Inventory list should be updated to include confirmation of contents or variations observed. Receiving person(s) should sign and date inventory worksheet to preserve chain of custody.

Evidentiary Retention

1. All original evidence should be recorded, examined for damage or observed anomalies, and stored in a protective safe. This safe should only be accessible by authorized incident responders and provide compartmentalized storage to accommodate multiple investigations.

2. All original documentation relating to a particular investigation should be stored in the safe with its corresponding evidence. Original evidence and documentation should never be modified once stored in this manner.

3. A log should be maintained to ensure chain of custody is maintained during and after an investigation. This log should include verification of removal, access, and submissions to the safe.

4. The safe should be located in a protected area with acceptable means for authentication and access control. A record of access should be maintained and preserved indefinitely.

5. This room should provide reasonable protection from various forms of damage such as fire, water, heat, cold or humidity.

6. The safe should be secured to either the floor or wall if it can be removed from the premises by reasonable means.

Evidentiary Retention (Cont'd.)

7. All investigative and analytical work should be performed on forensically obtained copies of original evidence, which should be appropriately labeled as such and stored along with it's original counterpart when not being used.

8. Evidence should always be removed from workspaces when not in use, even when working in a secured setting. This may prevent unauthorized persons from accidentally coming in contact with evidence.

9. Electronic evidence should never come in contact with magnetic devices or fields. Care should be taken to ensure that tools and other items used to access these devices are intended for electronic use as many possess magnetic properties.

10. All electronic copies may be stored to various forms of optical or magnetic mediums for backup and archival purposes once an investigation ends.

11. Archival and backup evidence may be stored at secured and authorized facilities after an investigation ends. This will ensure available space for future incidents, and allow for long-term retention if further analysis is required. Proper record retention requirements should be determined but is specifically outside of the scope of this document.